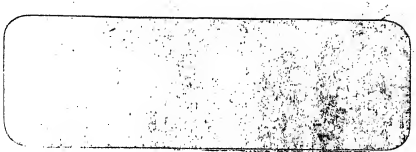
EXHIBIT 1

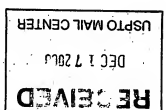
Organization_____ Bldg./Room_____
U. S. DEPARTMENT OF COMMERCE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
IF UNDELIVERABLE RETURN IN TEN DAYS

OFFICIAL BUSINESS

UNITED STATES POSTAGE
PITNEY BOWES
02 1M $ 01.68⁰
0004244939 DEC 10 2008
MAILED FROM ZIPCODE 22314

AN EQUAL OPPORTUNITY EMPLOYER





AF / IFW

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,678	02/19/2004	Daniel J. Zigmond	MS306815.01	5266

69316 7590 12/09/2008

MICROSOFT CORPORATION
ONE MICROSOFT WAY
REDMOND, WA 98052

EXAMINER	
FISCHER, ANDREW J	
ART UNIT	PAPER NUMBER
3621	
MAIL DATE	DELIVERY MODE
12/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/782,678
Filing Date: February 19, 2004
Appellant(s): ZIGMOND ET AL.

William J. Breen, III
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed February 26, 2007 appealing from the Office action mailed August 28, 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is not correct. This Examiner's Answer contains new grounds of rejection.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2003/0028488 A1	Mohammed et al	2-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis

for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -
(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21 (2) of such treaty in the English language.

Claims 1-42, are rejected under 35 U.S.C. 102(e) as being anticipated by Mohammed et al U.S. patent Application Publication No. 2003/0028488 AI.

As per **claim 1 and 10**, Mohammed et al discloses a method comprising: forming a request by a client to access encrypted content, wherein:

the request includes a persistent license for communication to a licensing server (see figs. 5 and 13; 0017; 0155; 0156); and

the persistent license includes a key that is encrypted such that the key is not accessible by the client (0016; 0017); and

receiving a license in response to the request, wherein the received license includes the key that is:

accessible by the client (0016); and

for accessing the encrypted content (0016; 0017; 0018).

As per **claim 2**, Mohammed et al further discloses a method, further comprising: forming an initial request for: communication to the licensing server (fig. 1 and 5; 0135; 0137); and storing encrypted content by the client (0116);

receiving the persistent license at the client in response to the initial request (fig. 1, 5, 6, 7 and 13; 0135); and

storing the encrypted content and the persistent license by the client (see figs. 1, 5 and 14; 0185).

As per **claim 3**, Mohammed et al further discloses a method, further comprising: forming an initial request by another client for: communication to the licensing server (fig. 1 and 5; 0135; 0137); and

storing encrypted content by the other client (0116);

receiving the persistent license at the other client in response to the initial request (fig. 1, 5, 6, 7 and 13; 0135);

storing the encrypted content and the persistent license by the other client (see figs. 1, 5 and 14; 0185; 0130); and

obtaining the persistent license by the client from the other client (fig. 6).

As per **claim 4**, Mohammed et al further discloses a method, wherein the received license is a boundary license and the key is a boundary key, and further comprising:

decrypting a session license utilizing a client key to obtain a session key (see figs. 6 and 8; 0013; 0050; 0055; 0118; 0121);

decrypting the boundary license utilizing the session key to obtain the boundary key (see figs. 6 and 8; 0013; 0050; 0055; 0118; 0121);

decrypting a content license utilizing the boundary key to obtain a content key (0050; 0055; 0118; 0121);

and decrypting the encrypted content utilizing the content key (figs. 5 and 10).

As per **claim 5**, Mohammed et al further discloses a method, wherein:
the session license includes access rules for the client for a session initiated between the client and the licensing server (0002; 0009);
the boundary license includes access rules for the client for the encrypted content that is within a rights boundary in the encrypted content (0050); and
the content license includes access rules for the client for the encrypted content (0050).

As per **claim 6**, Mohammed et al further discloses a method, wherein:
the persistent license was encrypted using an asymmetric encryption algorithm (0079); and
the encrypted content, the boundary license, and the content license were encrypted using respective symmetric encryption algorithms (0050).

As per **claim 7**, Mohammed et al further discloses a method, further comprising:
decrypting a session license utilizing a client key to obtain a session key, wherein the session license includes access rules for a session initiated between the client and the licensing server (fig. 13; 0002; 0009; 0010);
decrypting the received license utilizing the session key to obtain a decrypted boundary license, wherein: the received license is an encrypted boundary license and the key within the boundary license is a boundary key (see figs. 6 and 8; 0013; 0050; 0055; 0118; 0121); and
the boundary license includes access rules for content within a rights boundary in the encrypted

content that is at least one of a television program and a television channel (0105); decrypting a content license utilizing the boundary key to obtain a content key, wherein the content license includes access rules for the encrypted content (0050; 0055; 0118; 0121); and decrypting the encrypted content utilizing the content key, wherein the encrypted content includes at least a portion of a television broadcast (0050; 0055; 0118; 0121; 0105).

As per **claim 8**, Mohammed et al further discloses a method, wherein the key is for decrypting the encrypted content (0050; 0079).

As per **claim 9**, Mohammed et al further discloses a method, wherein the encrypted content is streamed to the client (0070; 0072).

As per **claim 11 and 16**, Mohammed et al discloses a method comprising: forming a request by a client for communication to a licensing server, wherein the request is for storing encrypted content by the client (see figs. 1, 5 and 14; 0185; 0018; 0121; 0113; 0116); receiving a persistent license at the client in response to the request, wherein: the persistent license includes a key that is encrypted (0050; 0055; 0118; 0121);
the key, when decrypted, provides access to the encrypted content (0128);
the key is configured to be decrypted by the licensing server (0012; 0018; 0105; 0325; 0326); and
the client is not configured to decrypt the key from the persistent license (0016; 0017); and storing the persistent license and the encrypted content by the client (see fig. 7 and 14; 0118;

0121).

As per **claim 12**, Mohammed et al further discloses a method, further comprising:
forming a subsequent request by the client to access the stored content, wherein the subsequent request:
is for communication to the licensing server (see fig. 5; 0017; 0096; 0146; 0155; 0156); and
includes the persistent license (see fig. 5; 0017; 0096; 0146; 0155; 0156); and
receiving a second license at the client in response to the subsequent request, wherein:
the second license includes the key (0050; 0152; 0156); and
the second license is configured to be decrypted by the client such that the client obtains access to the key (0050; 0152; 0156).

As per **claim 13**, Mohammed et al further discloses a method, further comprising:
forming a subsequent request by another client to access the stored content, wherein the subsequent request:
is for communication to the licensing server (figs. 5, 6 7, and 13); and includes the persistent license (see fig. 5; 0017; 0096; 0146; 0155; 0156); and
receiving a second license at the other client in response to the subsequent request, wherein:
the second license includes the key (0017; 0096; 0146; 0155; 0156); and
the second license is configured to be decrypted by the other client such that the other client obtains access to the key (see fig. 5; 0017; 0096; 0146; 0155; 0156).

As per **claim 14**, Mohammed et al further discloses a method, wherein the encrypted content is streamed to the client (0070; 0072).

As per **claim 15**, Mohammed et al further discloses a method, wherein the license includes a certificate for verifying the licensing server by the client (0168; 0169; 0177; 0201).

As per **claim 17 and 22**, Mohammed et al further discloses a method comprising:
forming a first request for communication to a licensing server, wherein the first request is for storing encrypted content (see figs. 1, 5 and 14; 0185; 0018; 0121; 0113; 0116; 0155; 0156);
receiving a persistent license in response to the request, wherein the persistent license includes a boundary key (0050; 0055; 0118; 0121);
storing the persistent license and the content (see figs. 1, 5 and 14; 0185; 0130); forming a second request to access the encrypted content, wherein the second request includes the persistent license (see figs. 1, 5 and 14; 0185; 0018; 0121; 0113; 0116; 0155; 0156);
sending the second request to the licensing server (fig. 1);
receiving a boundary license in response to the second request, wherein the boundary license includes the boundary key (0013; 0050; 0055; 0118; 0121);
decrypting the boundary license using a session key to obtain the boundary key (see figs. 6 and 8; 0013; 0050; 0055; 0118; 0121);
decrypting a content license using the boundary key to obtain a content key (see figs. 6 and 10;

0013; 0050; 0055; 0118; 0121); and

decrypting the encrypted content using the content key (figs. 5 and 10).

As per **claim 18**, Mohammed et al further discloses a method, wherein the forming of: the first request is performed by a first client (fig. 1); and the second request is performed by a second client (fig. 1).

As per **claim 19**, Mohammed et al further discloses a method, wherein the first and second requests are formed by a client (fig. 1).

As per **claim 20**, Mohammed et al further discloses a method, further comprising at least one of decoding the decrypted content and outputting the decoded content (see fig. 5).

As per **claim 21**, Mohammed et al further discloses a method, wherein: the persistent license was encrypted using an asymmetric encryption algorithm (0079); and the content, the boundary license, and the content license were encrypted using respective symmetric encryption algorithms (0050).

As per **claim 23**, Mohammed et al further discloses a client comprising: a processor (fig. 12); and memory configured to maintain: a persistent license including a key that is encrypted (fig. 4); and a playback application that is executable on the processor to: form a request to access encrypted content, wherein the request:

is for communication to a licensing server (fig. 13); and includes the persistent license (fig. 4; 0276); receive a response to the request that includes the key (0276); and access the encrypted content utilizing the key (fig. 3; 0016; 0276).

As per **claim 24**, Mohammed et al further discloses a client, wherein the key is for decrypting the encrypted content (fig. 10; 0151).

As per **claim 25**, Mohammed et al further discloses a client, wherein:
the memory is further configured to maintain a content license (fig. 4);
the key included in the persistent license is for decrypting the content license (fig. 1);
the content license includes a content key (fig. 1); and
the content key is for decrypting the encrypted content (figs. 1 and 10).

As per **claim 26**, Mohammed et al further discloses a client, wherein: the memory is further configured to maintain a content license (fig. 4);
the key included in the persistent license is fordecrypting the content license (fig. 1; 0096);
the content license includes a content key (fig. 1 and 3; 0100); the content key is for decrypting the encrypted content (figs. 1 and 10; 0100); and the playback application is executable to:
decrypt the content license using the key to obtain the content key (fig. 5 and 14; 0128); and
decrypt the content using the content key (figs. 1 and 10; 0100; 0128).

As per **claim 27**, Mohammed et al further discloses a client, wherein:

the memory is further configured to maintain a session license, a content license, and a client key (fig. 4);

the client key is for decrypting the session license (fig. 1 and 3; 0100); the session license includes a session key for decrypting the response (0100); the response is a boundary license (see figs. 6 and 10; 0013; 0050; 0055; 0118;

0121);

the key included in the response is a boundary key for decrypting the content license (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

the content license includes a content key (figs. 1 and 10; 0100; 0128); and the content key is for decrypting the encrypted content (figs. 1 and 10; 0100;

0128).

As per **claim 28**, Mohammed et al further discloses a client, wherein:

the memory is further configured to maintain a session license, a content license, and a client key (see fig. 1 and 4);

the client key is for decrypting the session license (0100);

the session license includes a session key for decrypting the response (0100);

the response is a boundary license (see figs. 6 and 10; 0013; 0050; 0055; 0118;

0121);

the key included in the response is a boundary key for decrypting the content license (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

the content license includes a content key (fig. 1 and 3; 0100);

the content key is for decrypting the encrypted content (fig. 1 and 3; 0100); and

the playback application is executable to:

decrypt the session license using the client key to obtain the session key (0013; 0050; 0055; 0118; 0121);

decrypt the boundary license using the session key to obtain the boundary key (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

decrypt the content license using the boundary key to obtain the content key (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121); and

decrypt the content using the content key (figs. 1 and 10; 0100; 0128).

As per **claim 29**, Mohammed et al further discloses a client, wherein the playback application is further executable to: form an initial request for: communication to the licensing server (see figs. 6 and 13; 0017; 0155; 0156);

and

storing encrypted content by the playback application (fig. 4 and 14);

receive the persistent license in response to the initial request (see figs. 5, 6 and 7; 0050; 0055; 0118; 0121); and

store the encrypted content and the persistent license (see figs. 1, 5 and 14; 0185; 0130).

As per **claim 30**, Mohammed et al further discloses a client, wherein the playback application is further executable to form a request to obtain the encrypted content from another

client (see figs. 4, 5 and 14).

As per **claim 31**, Mohammed et al further discloses a client, further comprising a tuner configured to receive the encrypted content when streamed over a network (0070; 0072).

As per **claim 32**, Mohammed et al further discloses a client, wherein the license includes a certificate for verifying the licensing server (see fig. 10; 0168; 0169; 0177; 0201).

As per **claim 33**, Mohammed et al further discloses a system comprising:

a network (fig. 1 and 13);

a client including:

a persistent license having a key that is encrypted (fig. 1 and 4; 0016; 0017); and a playback application that is executable to:

form a request to access encrypted content, wherein the request includes the persistent license (see figs. 4, 5, 6 7 and 13);

receive a response to the request that includes the key (see figs. 4, 5, 6 7 and 13; 0016); and access the encrypted content utilizing the key (0050; 0055; 0118; 0121); and a licensing server including a licensing module that is executable to: receive the request including the persistent license (0276);

decrypt the persistent license to obtain the key (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121); and

form the response that includes the key for communication to the client over the network (see

figs. 6, 7 and 13; 0010).

As per **claim 34**, Mohammed et al further discloses a system, wherein: the client includes a content license (fig. 4);

the key included in the persistent license is for decrypting the content license (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

the content license includes a content key (figs. 1 and 10; 0100; 0128); and the content key is for decrypting the encrypted content (fig. 1 and 3; 0100).

As per **claim 35**, Mohammed et al further discloses a system, wherein: the client includes a content license (fig. 4, and 7);

the key included in the persistent license is for decrypting the content license (fig. 1 and 3; 0100);

the content license includes a content key (figs. 1 and 10; 0100; 0128); the content key is for decrypting the encrypted content (fig. 1 and 3; 0100); and the playback application is executable to:

decrypt the content license utilizing the key to obtain the content key (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121); and

decrypt the content utilizing the content key (fig. 1 and 3; 0100).

As per **claim 36**, Mohammed et al further discloses a system, wherein:

the client includes a session license, a content license, and a client key (see figs. 1 and 4);

the client key is for decrypting the session license (0100); the session license includes a session key for decrypting the response (0100); the response is a boundary license (see figs. 6 and 10; 0013; 0050; 0055; 0118;

0121);

the key included in the response is a boundary key for decrypting the content license (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

the content license includes a content key (figs. 1 and 10; 0100; 0128); and the content key is for decrypting the encrypted content (fig. 1and 3; 0100).

As per **claim 37**, Mohammed et al further discloses a system, wherein:

the client includes a session license, a content license, and a client key; the client key is for decrypting the session license (see figs. 1 and 4);

the session license includes a session key for decrypting the response (0100); the response is a boundary license ();

the key included in the response is a boundary key for decrypting the content license (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

the content license includes a content key (figs. 1 and 10; 0100; 0128); the content key is for decrypting the encrypted content (fig. 1 and 3; 0100); and the playback application is executable to:

decrypt the session license utilizing the client key to obtain the boundary key (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

decrypt the boundary license utilizing the session key to obtain the boundary key (see figs. 6 and

10; 0013; 0050; 0055; 0118; 0121);

decrypt the content license utilizing the boundary key to obtain the content key (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

decrypt the content utilizing the content key (fig. 1 and 3; 0100); and

play the decrypted content (fig 5).

As per **claim 38**, Mohammed et al further discloses a system, wherein the key is for decrypting the encrypted content (0050; 0079).

As per **claim 39**, Mohammed et al further discloses a system, wherein the persistent license is encrypted with an asymmetric encryption algorithm and the server includes a server private key for decrypting the persistent license (0050; 0079).

As per **claim 40**, Mohammed et al further discloses a system, wherein the playback application is further executable to: form an initial request for: communication to the licensing server (figs. 13); and storing encrypted content by the playback application (see figs. 1, 5 and 14;

0185);

receive the persistent license in response to the initial request (see figs. 1, 5, 7, 13 and 14; 0185); and

store the encrypted content and the persistent license (see figs. 1, 5 and 14;

0185).

As per **claim 41**, Mohammed et al further discloses a system, wherein the playback application is further executable to form a request to obtain the encrypted content from another client (fig. 6).

As per **claim 42**, Mohammed et al further discloses a system, wherein the encrypted content is streamed to the client over the network (0010; 0070; 0072).

NEW GROUNDS OF REJECTION

Claim Rejections - 35 USC § 101

Claims 1-21 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Based on Supreme Court precedent[1] and recent Federal Circuit decisions, a §101 process must (1) be tied to another statutory class (such as a particular apparatus) or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. See *In re Bilski*, 88 USPQ2d 1385 (Fed. Cir. 2008) (en banc).

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps.

To meet prong (1), the method step should positively recite the other statutory class (the thing or product) to which it is tied. This may be accomplished by having the claim positively recite the

[1] See also *Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 437 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972); *Cochrane v. Deener*, 94 U.S. 780, 787-88 (1876).

machine that accomplishes the method steps. Alternatively or to meet prong (2), the method step should positively recite identifying the material that is being changed to a different state or positively recite the subject matter that is being transformed.

In this particular case, the claims fail prong (1) because the method steps are not tied to a machine and can be performed without the use of a particular machine. Additionally, the claim(s) fail prong (2) because the method steps do not transform the underlying subject matter to a different state or thing. For example, the first method step of claim 1 recites "forming a request by a client to access encrypted content", but fails to identify a machine that performs the "forming a request".

(10) Response to Argument

With respect to **claim 1**, Appellant argues that Mohammed does not disclose the features as recited in claim 1. Specifically that Mohammed does not show the communication of an encrypted key from the client, which is then decrypted by the licensing server and communicated back to the client to access the content.

In response, Examiner respectfully disagrees and submits that Mohammed discloses all of the recited features of claim 1 as shown in the rejection above and on the attached chart. Mohammed further shows the communication of an encrypted key from the client, which is then decrypted by the licensing server and communicated back to the client to access the content (0016; 0017). As shown in the chart, Mohammed made it clear that:

"A license request also includes an identification of the digital content for which a license is requested and a key ID that identifies the decryption key associated with the requested digital content."

It is with the client identification information(persistent license) together with the key ID that is sent to the license server that was also used for the license 16 and decryption key that was sent back to the client and subsequently used to decrypt the digital content. In nowhere did Mohammed disclose that the above cited key ID or decryption key that is transmitted by the client in forming its request for a license is accessible to the client. The key is not decrypted by the client rather the key is used only to request the license from the license server. Therefore the rejection of claim 1 is appropriate and claim 1 is not patentable over Mohammed.

As per **claims 2-10**, Appellant argues depend either directly or indirectly from claim 1 and are allowable as depending from the allowable base claim or on the alternative are allowable for their own recited features.

In response, Examiner respectfully disagrees and asserts that these claims are neither allowable being dependent on claim 1 nor allowable for their own recited features.

With regards to **claim 11**, Appellant argues is allowable based on similar reasoning as presented in claim 1. Specifically, claim 11 recites: "the persistent license includes a key that is encrypted"; "the key, when decrypted, provides access to the encrypted content"; "the key is configured to be decrypted by the licensing server'; and "the client is not configured to decrypt the key from the persistent license."

In response, Examiner respectfully disagrees with Appellant's characterization. As shown in the attached chart, the Examiner asserts that Mohammed does discloses all the recited feature

of claim 11 thus: "the persistent license includes a key that is encrypted" (see 0016; 0017; 0050; 0055; 0118; 0121); "the key, when decrypted, provides access to the encrypted content" (see 0016; 0017; 0128); "the key is configured to be decrypted by the licensing server" (see 0012; 0016; 0017; 0018; 0105; 0325; 0326); and "the client is not configured to decrypt the key from the persistent license" (see 0016; 0017). Since Mohammed discloses all the features of claim 11, claim 11 is not allowable over Mohammed.

As per **claims 12-16**, Appellant argues depend either directly or indirectly from claim 11 and are allowable as depending from the allowable base claim or on the alternative are allowable for their own recited features.

In response, Examiner respectfully disagrees and asserts that these claims are neither allowable being dependent on claim 11 nor allowable for their own recited features.

With regards to **claim 17**, Appellant argues is allowable based on similar reasoning previously mentioned with respect to claim 1 as well as its own recited features. In particular that Mohammed does not disclose: "receiving a persistent license in response to the request, wherein the persistent license includes a boundary key; storing the persistent license and the content; forming a second request to access the encrypted content, wherein the second request includes the persistent license; sending the second request to the licensing server; receiving a boundary license in response to the second request, wherein the boundary license includes the boundary key.

In response, Examiner respectfully disagrees and submits that claims 17 is not allowable for similar reasoning advanced with respect to claim 1 above. Specifically Mohammed does disclose: receiving a persistent license in response to the request, wherein the persistent license

includes a boundary key (decryption key) (0050; 0055; 0118; 0121); storing the persistent license and the content (see figs. 1, 5 and 14; 0185; 0130); forming a second request to access the encrypted content, wherein the second request includes the persistent license (see figs. 1, 5 and 14; 0185; 0018; 0121; 0113; 0116; 0155; 0156); sending the second request to the licensing server (fig. 1); receiving a boundary license in response to the second request, wherein the boundary license includes the boundary key (0013; 0050; 0055; 0096; "... Preferably such transmitted license includes the decryption key for decrypting the digital content 12...; 0118; 0121). Thus, claim 17 is not allowable over Mohammed as shown in the rejections and as shown in the chart.

As per **claims 18-22**, Appellant argues depend either directly or indirectly from claim 17 and are allowable as depending from the allowable base claim or on the alternative are allowable for their own recited features.

In response, Examiner respectfully disagrees and asserts that these claims are neither allowable being dependent on claim 17 nor allowable for their own recited features.

With regards to **claim 23**, Appellant argues is allowable based on similar reasoning previously mentioned with respect to claim 1 as well as for its own recited features. In Particular Claim 23 recites: a client having "a persistent license including a key that is encrypted; and a playback application that is executable on the processor to: form a request to access encrypted content, wherein the request: is for communication to a licensing server; and includes the persistent license; receive a response to the request that includes the key; and access the encrypted content utilizing the key.

In response, Examiner respectfully disagrees and submits that claims 23 is not allowable for similar reasoning advanced with respect to claim 1 above nor for its own recited features. Thus, claim 23 is not allowable over Mohammed as shown in the chart as well as in the rejections.

As per **claims 24-32**, Appellant argues depend either directly or indirectly from claim 23 and are allowable as depending from the allowable base claim or on the alternative are allowable for their own recited features.

In response, Examiner respectfully disagrees and asserts that these claims are neither allowable being dependent on claim 23 nor allowable for their own recited features.

With regards to **claim 33**, Appellant argues is allowable based on similar reasoning previously mentioned with respect to claim 1 as well as its own recited features.

In response, Examiner respectfully disagrees and submits that claims 33 is not allowable for similar reasoning advanced with respect to claim 1 above. Thus, claim 33 is not allowable over Mohammed as shown in the chart as well as in the rejections.

As per **claims 34-42**, Appellant argues depend either directly or indirectly from claim 33 and are allowable as depending from the allowable base claim or on the alternative are allowable for their own recited features.

In response, Examiner respectfully disagrees and asserts that these claims are neither allowable being dependent on claim 33 nor allowable for their own recited features.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

This examiner's answer contains a new ground of rejection set forth in section **(9)** above. Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one of the following two options to avoid *sua sponte* **dismissal of the appeal** as to the claims subject to the new ground of rejection:

(1) **Reopen prosecution.** Request that prosecution be reopened before the primary examiner by filing a reply under 37 CFR 1.111 with or without amendment, affidavit or other evidence. Any amendment, affidavit or other evidence must be relevant to the new grounds of rejection. A request that complies with 37 CFR 41.39(b)(1) will be entered and considered. Any request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) **Maintain appeal.** Request that the appeal be maintained by filing a reply brief as set forth in 37 CFR 41.41. Such a reply brief must address each new ground of rejection as set forth in 37 CFR 41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 CFR 41.37(c). If a reply brief filed pursuant to 37 CFR 41.39(b)(2) is accompanied by any amendment, affidavit or other evidence, it shall be treated as a request that prosecution be reopened before the primary examiner under 37 CFR 41.39(b)(1).

Extensions of time under 37 CFR 1.136(a) are not applicable to the TWO MONTH time period set forth above. See 37 CFR 1.136(b) for extensions of time to reply for patent

applications and 37 CFR 1.550(c) for extensions of time to reply for ex parte reexamination proceedings.

Respectfully submitted,

/Jacob C. Coppola/

Examiner, Art Unit 3621

Vincent Millin
Appeals Practice Specialist

ANDREW J. FISCHER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

A Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing below:

WYNN W. COGGINS
TECHNOLOGY CENTER DIRECTOR

APPEAL CHART

SERIAL NO. 10/782678
Examiner: Charlie Agwumezie
Art Unit 3621

Phrase No.	Claim Description	**Mohammed et al U.S. Pub. No. 2003/0028488**
Claims 1	**forming a request by a client**	Client (computing device 14) request access to encrypted content 12 (package 12p) see fig. 5
	the request includes a Persistent license	the request includes a user identification or user ID including a key (0017)
	for communication to a licensing server	the request information transmitted to the license server 24. (0017; 0018; 0154)
	the persistent license includes a key that is encrypted such that the key is not accessible by the client	the request includes Key ID that identifies the decryption key (KD) (0017; 0151)
	receiving a license in response to the request	receiving "license 16" by user computing device 14 (0096)
	wherein the received license includes the key	the received "license 16" includes a decryption key (0096)
	accessible by the client	accessible by the client 14 for decrypting the digital content 12 (0096)
	for accessing the encrypted content	for decrypting the digital content 12
Independent Claims 11	forming a request by a client	Client (computing device 14) request access to encrypted content 12 (package 12p) see fig. 5
	for communication to a licensing server	request information transmitted to the license server 24. (0017; 0018; 0154)
	wherein the request is for	Digital content 12 or package 12p

	storing encrypted content by the client	(0084)
	receiving a persistent license at the client in response to the request	receiving "license 16" by user computing device 14 (0096)
	wherein the persistent license includes a key that is encrypted	the received "license 16" includes a decryption key (0096)
	the key, when decrypted, provides access to the encrypted content	when the key is decrypted provides access to digital content 12 (0096)
	The key is configured to be decrypted by the licensing server	the licensing server decrypts the Key (0017; 0018)
	the client is not configured to decrypt the key from the persistent license	the Black box server 26 decrypts the key See fig. 1
	storing the persistent license and the encrypted content by the client	License Store 38, and package 12p See fig. 4
Independent Claim 17	forming a first request for communication to a licensing server	Client (computing device 14) request access to encrypted content 12 (package 12p) see fig. 5
	wherein the first request is for storing the encrypted content	Digital content 12 or package 12p fig. 5
	receiving a persistent license in response to the request	receiving "license 16" by user computing device 14 (0096)
	wherein the persistent memory includes a boundary key	the received "license 16" includes a decryption key (0096)
	storing the persistent license and the content	"The license store 38 stores licenses 16 received by the DRM system 32 for corresponding digital content 12..." (0130)
	forming a second request to access the encrypted content	Attempt to render 501 (See fig. 5B)
	wherein the second request includes the persistent license	Check for valid enabling license 16 in license store 38 (see fig. 5B)
	Sending the second request to the licensing server	No valid license? Acquire license 16 from License server 24 (see fig. 5)

	receiving a boundary license in response to the second request	receiving "license 16" by user computing device 14 (0096)
	wherein the boundary license includes the boundary key	the received "license 16" includes a decryption key (0096)
	decrypting the boundary key using a session key to obtain the boundary key	Decryption key (0017)
	decrypting content license using boundary key to obtain content key	Content key (0276)
Independent Claim 23	a processor	Computer 120 (see fig. 12)
	a persistent license including a key that is encrypted	the received "license 16" includes a decryption key (0096)
	a playback application	Rendering Application 34 (see fig. 4)
	form a request to access encrypted content	Client (computing device 14) request access to encrypted content 12 (package 12p) see fig. 5
	wherein the request is for communication to a licensing server	request information transmitted to the license server 24. (0017; 0018; 0154)
	includes the persistent license	User id (0017)
	receive a response to the request that includes the key	the received "license 16" includes a decryption key (0096)
	access the encrypted content utilizing the key	Render content 12 (see fig. 5B)
Independent Claim 33	A network	A Network LAN 151 (0038)
	a client	Computing device 14
	a persistent license having a key that is encrypted	User id having a Key ID (0017)
	A playback application	Rendering Application 34 (see fig. 4)
	forming a request to access encrypted content	Client (computing device 14) request access to encrypted content 12 (package 12p) see fig. 5

	wherein the request includes a persistent license		the request includes a user identification or user ID including a key (0017)
	receive a response to the request that includes the key		the received "license 16" includes a decryption key (0096)
	access the encrypted content utilizing the key		Render content 12 (see fig. 5B)
	a license server		License server 24
	receive the request including a persistent license		the request includes a user identification or user ID (0017)
	decrypt the persistent license to obtain a key		Decryption key (0017)
	form the response that includes the key for communication to the client over the network		the received "license 16" includes a decryption key (0096)